STRENGTHENING PROGRAM FOR NUCLEAR CYBER SECURITY AT NUCLEAR FACILITIES

Dikdik Sidik Purnama[1, 3*], Mokhamad Hendayun[5], Barito Mulyo Ratmono[4], Satriani Aga Pasma[3], Poppy Setiawati Nurisnaeni[3], Rahmat Khatib Purnama[2, 3]

[1]*Research Center of Radiation Detection Technology and Nuclear Analysis, Nuclear Research Organization, National Research and Innovation Agency of Indonesia*

[2]*Directorate of nuclear facility management, National Research and Innovation Agency of Indonesia (Tamansari Street No. 71 Bandung 40132)*

[3]*Department of Medical Intelligence, State Intelligence College of Indonesia*

[4]*Department of Technology Intelligence, State Intelligence College of Indonesia (Sumur Batu, Babakan Madang, Kabupaten Bogor, Jawa Barat 16810)*

[5]*Department Informatic Engineering, Langlangbuana University (Karapitan Street No.116 Bandung 40261)*

**** Corresponding author:***

e-mail: dikdiksp@gmail.com

Received: 03-01-2023
Revision Received: 18-01-2023
Accepted: 05-04-2023

DOI : 10.17146/jstni.2022.23.2.6785

Keywords: *nuclear facility, cyber security, cyber-terrorism.*

Abstract *Threats to the safety and security of a facility could target the physical also cyber infrastructure aspects. Critical facilities such as nuclear facilities use cyber-physical systems in their operation has vulnerabilities. Nuclear facilities in Indonesia may become targets of cyberterrorism because there have been incidents of attacks in several countries related to nuclear terrorism for specific purposes that threaten the safety and security operations of the nuclear facilities. Similar threats may occur at other nuclear facilities as well as nuclear facilities in Indonesia. The purpose of this study is to propose a nuclear cybersecurity program with a qualitative approach to attract more attention in supporting the anticipation of increasing cybersecurity threats at nuclear facilities. The program was proposed based on the description of terms in nuclear safety and security and literature studies describing incidents of nuclear cyberterrorism attacks in the past. A cyber nuclear security program has been proposed through stakeholder collaboration, resource support, and capacity building for the ongoing nuclear security program.*

INTRODUCTION

The threat of nuclear terrorism has become a widespread concern for nuclear safety and security. Nuclear terrorism may occur not only against the physical target of the facility but also in the information technology systems used in the facility. Instrumentation and control of nuclear facilities are changing from analog devices that have relatively poor performance and maintenance difficulties to digital devices (1)(2). A variety of modern digital and cyber-physical systems are becoming the backbone for smart infrastructures such as smart facilities for medical appliances, power plants, etc. (3). The potential of cyber-attacks has escalated into a serious threat to nuclear facilities because of the digitalization of instrumentation and control systems through the adoption of the opened information technology system. Their safety and security cannot be guaranteed against possible cyber-attacks. Even when safety, control, and monitoring system operate in strictly controlled access environments, cyber threats to industrial control systems including nuclear facilities, have become real (4). Various events that lead to disturbances and are even categorized as acts of cyber terrorism have happened at various nuclear facilities. According to reports, the incidents happened in several countries such as the United States (5), Iran (6)(7), Germany (8)(9), and South Korea (1)(10)(11).

At critical facilities such as nuclear reactors or nuclear materials facilities, safety and security are the most important consideration. They cannot be separated from each other, because insecurity at a nuclear facility could lead to serious hazards such as nuclear accidents (12). Nuclear facilities in the world that have nuclear materials and equipment associated with the nuclear sector are generally owned and operated by government and private institutions and must be tightly regulated. It was also an obligation to comply with international nuclear security regulations.

At present, Indonesia has three nuclear facilities that were operated to support the research and development of nuclear technology. In the field of nuclear reactors, its research and development be more sophisticated by involving control systems based

on information systems technology and may raise vulnerability. It is important to make the secured operation through the nuclear cyber security program for the terror prevention strategy.

In this case, the regulatory body in various countries has regulated it through a regulatory and licensing approach with a framework that requires each license holder to comply with safety and security requirements to protect public health and safety, the environment, and supports national security. The owner or operator of the facility has established associations, working groups, or other mechanisms to facilitate the sharing of risk information and the exchange of information on best practices for the safety and operational security of nuclear facilities beyond the required regulations. However, the regulatory agency intensively only focuses on the physical aspect, so no regulatory system has been found that set explicitly safety and security objectives related to cyberinfrastructure that is applied in facilities associated with the nuclear field. According to the framework proposed by Bowsher et al., radiological and nuclear information became the domain of Medical Intelligence (13). In this study, we suggest constructs for a nuclear cybersecurity program involving an intelligence role.

METHODS

The methodology used in this study was a qualitative method, including describing the terms in nuclear safety and security and types of cyber-attacks, as well as studying literature to compile a list of events associated with cyber-attacks on nuclear facilities that have happened. In addition, this study compares the characteristics of the risks in the form of traditional terror attacks, cyber terror attacks, and threats in the context of security conditions. Furthermore, a nuclear cyber security program is suggested that involves the role of an intelligence agency to anticipate or prevent the threat of cyber nuclear attacks at nuclear facilities.

RESULTS AND DISCUSSION

Sources of threats at Nuclear Facility

In terms of safety and security as critical infrastructure, the following are examples of various sources of threats or intrusions that may happen in nuclear facilities:

1. Natural disasters: Disasters are a source of threat from external factors, such as earthquakes, landslides, tsunamis, and so on that can cause severe damage to operational systems and fail the emergency safety equipment systems of nuclear facilities which are categorized as critical infrastructure. In general, these threat risks have been considered long before and during construction and are included in the infrastructure maintenance program including the vulnerability of infrastructure and human resources involved in its operations.
2. Vulnerability of infrastructure and human resources aspects: Generally, the validity period of an operation permit for the facility, especially a nuclear reactor, is up to 40 years. Moreover, they run into aging risk factors, both in terms of infrastructure and workers. There is also a risk of declining skills and competencies of workers, so their upkeeping and development are needed.
3. Terrorism, sabotage, or deliberate act: nuclear facilities have the potential to become targets of sabotage and terror by using various means and equipment, for example, traditional weapons or advanced remote-controlled weapons causing destruction, damage, safety malfunctions, radiation contamination consequences to the surrounding community, loss of life, injury, or disability.
4. Cyberattacks: Almost all technological systems implemented at nuclear facilities are generally based on computer software controls connected to an intranet or internet network. This is a very open loophole as a vulnerability, which provides an opportunity for increasingly sophisticated hackers to maliciously control the computers and major equipment systems or other equipment systems for espionage, data theft, destruction, or interference with network-based systems using weapons. cyberspace such as malware, worms, or computer viruses. In the case of a severe attack, the attack can disrupt or destroy the control system which will be fatal to the safety and operational security of the nuclear facility.

Reports of Cyber Attacks Targeting Nuclear Facilities

The following is a descriptive report on events related to cyber-nuclear terrorism that occurred in several places:

1. Worm Infection on The United States Nuclear Power Plants Network Server Computer (5)

In 2003, the Microsoft SQL Slammer worm infected a computer network server at the Ohio Davis-Besse nuclear facility. This infection

increases data traffic flow on the network site, interrupting the availability of data supply on the security system parameter display for several hours. However, there are no consequences that threaten the nuclear power plant operation. Based on an investigation report by local regulatory agencies, that was the contractor set up an unprotected computer connected to his company's network, and this connection allowed the Worm to reach the nuclear power plant's networks.

In 2006, the Browns Ferry nuclear power plant located on the Tennessee River was forced to manually shut down due to two reactor recirculation pumps malfunctions. Further investigation revealed that the variable frequency drive (VFD) controller was unresponsive and a failure of the condensate demineralization controller, equipped with a redundant dual system programmable logic controller (PLC) connected to an integrated computer system network. It was discovered later that this failure was caused by excessive data traffic flow on the computer network system integrated into the facility. However, an investigation could not be carried out conclusively to determine whether the cause of the problem was PLC failure or excessive network traffic resulting in the VFD controller becoming unresponsive. However, the local regulatory agency states that some vulnerabilities could not be determined whether an unresponsive system followed by network traffic overload and PLC failure.

2. Stuxnet Worm Attacks Iranian Nuclear Plant Staff Computers

In 2010, the Stuxnet computer worm was identified by Virus-BlokAda belong to a Belarus-based security company. Stuxnet is a specially created and engineered application, advanced technology, and part of a complex cyber weapon consisting of dropper and payload parts: 1) virus spread based on vulnerabilities inherent with the Windows platform, and 2) attacks on surveillance control systems and data acquisition (SCADA) focused on WinCC and PCS7 from Siemens PLC systems (7). This is a sign that the Stuxnet targeting system made by German company Siemens has reached out to equipment systems linked to Iran's nuclear program. Speculation has emerged that there is a West concern that Iran's goal is nuclear weapon generating. Although, Iran says that its nuclear program is only intended for welfare purposes. Malicious computer code designed to take over industrial sites such as power plants has also appeared in India, Indonesia, and the United States. However, the highest prevalence happened in Iran.

European digital security firm Kaspersky Labs said the attack be carried out "with state support" only. Some Western experts said its complexity means that the code could be created on a "country" scale only. Stuxnet was designed to target weaknesses in Siemens systems to manage water supplies, oil rigs, power plants, and other utilities. It is believed to be the first Worm designed to target a major infrastructure facility. Mahmoud Liayi, head of the information technology board at the industry ministry, told the state-run Iran Daily newspaper, saying that "an electronic warfare attack has been launched against Iran".

Iran asserts that the Stuxnet attack resulted in the forced termination of several Natanz uranium enrichment centrifuge facilities in its nuclear program. It was reported by the Iranian website that it appears that Israel confirmed it was behind the attack. However, the operating system at the Bushehr facility, which will be running online in a few weeks, was not damaged, according to project manager Mahmoud Jafari. The fact that Stuxnet has been detected on staff personal computers will not be affected due to plans to keep the Bushehr facility operational. Experts team has attempted to remove this malware from several affected computers and has infected about 30,000 IP addresses in Iran.

3. Cyber-terror at a Nuclear Power Plant in South Korea.

Cyber terror at nuclear power plants (NPP) generated many security concerns from the December 2014 incident against Korea Hydro & Nuclear Power Co. Ltd. (KHNP) South Korean nuclear power plant (10). At the attack, at least three reactors were shut down on Christmas day then people were asked to stay away from those facilities (10). But in fact, there was no attack on nuclear power plants or other nuclear facilities in South Korea. The hackers showed several pictures of the facility and recordings of telephone conversations between the Korean president and the UN Secretary-General, then demanded money (11).

Cyber terror in nuclear facilities is associated with discoveries where potential losses could be calculated. In the case of cyber terror, psychological emergence becomes mostly calculated compared to other forms of physical terror. Therefore, economic losses appeared because of economic activity stagnation. At that time, many employees were overloaded all

Christmas. The people's ordinary life around the nuclear facility was disrupted because it was stopped due to face the possible consequences of the terror attack (11).

4. Virus Attack on German Nuclear Power Plants (9)

In 2016 a computer virus infected the PC used at the Rheinisch-Westfälisches Elektrizitätswerk (RWE) German nuclear power plant. Viruses on office computers and the systems used to model movement find nuclear fuel rods. Viruses on fuel rod system models and 18 USB sticks were found as removable data stores on computers. Staff discovered the virus as they prepared to upgrade the computerized control system for the Block B facility, which did not generate electricity during scheduled maintenance. More than 1,000 computers were inspected for cleaning up and also increased its security controls.

Among the existing viruses, there were two well-known malicious programs named W32. Ramnit and Conficker. Ramnit debuted in 2010 and is a remote access tool to steal data. While Conficker started in 2008 and aims to retrieve login names and financial data. Due to the infected system from the internet, neither Ramnit nor Conficker was not able to activate and steal data at the facility.

Director of Intelligence State Agency, James Clapper said, "It was not an attack because it was completely passive and did not cause any destruction or any kind of effect. No data destruction or data manipulation. It was just stolen." Disruption was the term used to distinguish non-destructive attacks such as those against Sony Corp. in 2014. Whereas Stuxnet's attacks on Iran's program would be considered destructive.

German power company RWE said the infection did not cause a significant threat because the control system was not connected to the internet, so the virus could not be activated. No system is directly involved in controlling the infected reactor, so there is no threat to the people because of its computer infection.

Safety and Security Aspects for Critical Infrastructure

Table 1 describes the characteristics of threats by types and sources, while Table 2 describes the types of cyber-attack modalities and their possibilities.

Tabel 1. Characteristic of Threats

Item	Traditional terrorism	Cyber-terrorism	Accident or disaster
Subject	Person	Person	Person, nature
Sign	Hard to detect	Could be detected	Could be detected or predicted
Tendency	Existed	Existed	Existed
Frequently	Rarely	Progressively	Rarely
Resources	Traditional weapon	Cyber weapon	
Impact	Generally bad (casualties, injuries, and material losses)	Uncertain (physical and infrastructure damage, could lead to accidents due to malfunction of the facility's safety and security system)	Generally bad (casualties, injuries, and material losses)
Anticipatory strategy	Detect, deter, delay, response	Prevent, detect, response	Forecast, prevent, detect, response

T**abel 2. Kinds of Cyber Attack Modality and Their likelihood**

Kinds	Definition	Likelihood	Actors
Reconnaissance attacks	Attacks to map computer systems and services for data theft	Very likely	Internal personnel or contract workers
Access attacks	Attacks to devices for unauthorized access	Very likely	Internal personnel or contract workers
Denial of service (DOS)	Attacks to make computer or memory resources too busy or full for requests to handle, thereby	Very likely	Internal personnel or contract workers

Kinds	Definition	Likelihood	Actors
	denying authorized users access to the system machine		
Active attacks	Attacks by transmitting data to all parties as a liaison that allow severe impact	Very likely	External personnel
Attacks in MANET	Attacks aimed at slowing or stopping the flow of information between nodes	Very likely	External personnel
Attacks on WSN	Attacks that prevent sensors from detecting and transmitting information over the network	Very likely	External personnel
Passive attacks	Attacks with the primary purpose of snooping without database interfering	Likely	External personnel
Malicious attacks	Deliberate attack for harm causing a large-scale disturbance	Likely	External personnel
Non-malicious attacks	Accidental attacks due to handling or operational errors with small losses	Likely	External personnel
Cyber crime	Cyber use for crime	Likely	External personnel
Cyber espionage	The use of cyber to target reconnaissance for specific purposes	Likely	External personnel
Cyber terrorism	The use of cyber for acts of terror causes victims	Unlikely	External personnel
Cyber war	Use of cyber for tactical wars	Very unlikely	External personnel

The modality of cyber-attacks associated with cyber terrorism on nuclear facilities in Indonesia has never been reported, so the possibility was stated as unlikely. However, it does not rule out the possibility of increasingly sophisticated technological developments of the reactor technology instrumentation towards digitalization and automation of the control systems so that the opportunities for these attacks could be more open. Moreover, if it magnified by other factors as well as social and environmental factors.

Usually, the attack actors, previously called hackers, will synchronize to infect the system. Synchronization steps are carried out to steal information and then bring it to the expected destination so that the attacker will infect the system effortlessly through the organized attack forms or methods that could be used. The Logical and organized methods were used to lead them to obtain more effective and efficient results. The attack would be arranged in a perfectly designed sequence such that the damage is quite a severity (14)(15).

The existence of facilities classified as critical infrastructure such as nuclear facilities include the risk of the vulnerabilities described above. The increase in nuclear and radioactive materials used in Indonesia means that nuclear facilities such as nuclear reactors which use and produce radioactive material must be critical and vital at the same time, because of their benefits as well as safety and security aspects. As an illustration, based on data taken up to 2016, the number of permit holders to operate facilities, equipment and materials related to the nuclear sector in Indonesia has reached 15,000. That is, the large number of nuclear technologies used in Indonesia as part of the mastery of technological progress to support industrial activities and economic progress in Indonesia requires more attention to security and safety aspects.

The explanation above shows the importance of more intensive attention to the vulnerability of cyberinfrastructure at nuclear facilities to potential threats related to nuclear cyberterrorism in Indonesia.

Significant progress has been developed in the traditional nuclear security area. However, practices of traditional nuclear security only focused on preventing attacks on physical aspects such as regulating and securing gates or door access and placing safeguards as a precautionary measure against the theft of nuclear material for unauthorized use and nuclear facilities sabotage or unauthorized access to the control system of the nuclear facility. Meanwhile, the probability of threats along with advances in information technology uses could become increase and there is no guarantee that the systems operate appropriately as well as planned if it attacked by sophisticated cybercriminal actors. Ultimately, all countries including Indonesia are vulnerable to nuclear cyberterrorism.

Even though the cyber terrorism threat at nuclear facilities is considered unlikely, cyber-attacks are possible. For example, hackers act to turn off the security systems at nuclear facilities or nuclear fuel storage facilities, thus opening access to terrorists seeking nuclear material for nuclear weapons production. In addition, the hacker's trying to turn off the safety and security system control caused the failure system and then the leakage of radioactive material and contamination and radiation exposure to the public.

Technically, the global capacity to countermeasure the nuclear cyberterrorism threat is still limited and examined. This is also exacerbated by regional inequalities in cybersecurity expertise in some sectors. Therefore, these programs need to be continuously developed and strengthened. The recommendations for corrective and strengthening actions in nuclear cyber security and countermeasure capabilities include 1) collaboration with the expert community and stakeholders for the frameworks and technical guidelines development and 2) a looking forward approach to securing nuclear facilities from all the threats forms as well as nuclear cyber terrorism. At least it becomes the real action to pay attention and awareness of the importance of cyber security for critical infrastructure.

Strengthening for Nuclear Cyber Security at Nuclear Facility

Figure 1 following was a program scheme that could be implemented related to strengthening nuclear cyber security.

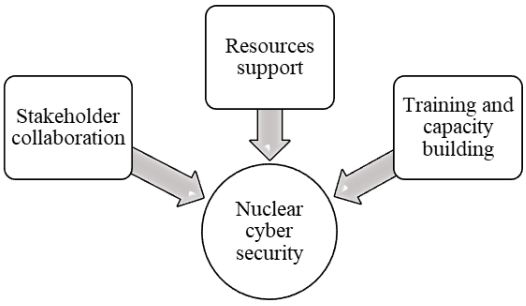

Figure 1. Scheme of strengthening for nuclear cyber security at nuclear facility

1. Stakeholder Collaboration

This action could be performed involving cyber security institutions' role with partner institutions in the nuclear sector, as well as other related institutions that define the same goals and objectives towards supporting the security posture and resilience of nuclear facilities, within involves intelligence agencies, policymakers, regulatory bodies, law enforcement agencies, military, and owners or operators of facilities. In addition to effectiveness, it could be done by forming a working group or task force for regularly discuss, information sharing, and developing technical instruments, guidelines, and products. This group intensively plans, implements, and carries out its functions across sectors regarding nuclear security and resilience programs. In this case, intelligence agencies or security agencies may hold confidential information through regular meetings to share up-to-date risk information with representatives at nuclear facilities and identify vulnerabilities, cyber threats, and their consequences. Additional meeting agendas maybe also necessary.

2. Resources Support

The frameworks and guidelines for sharing the threats targeting critical infrastructure information explain how the information data could be shared in the middle of stakeholders, governments, facility owners, and operators. Intelligence agencies should be able to offer resources to assist facility owners or operators in managing the risk related, strengthening security, and performing threats response and countermeasures in the nuclear sector. For example, the existence of convenient risk analysis instruments software-based is needed for evaluation, performance improvement, and updating the plans periodically and sustainably. It can be used by owners and operators of nuclear facilities to assess and manage cybersecurity risks that are expected to improve the security aspects of their infrastructures.

3. Training and Capacity Building

Training on critical infrastructure awareness is required, as well as web-based security, security in the workplace, insider threats mitigation, activity monitoring, theft prevention, and other cybersecurity related. Seminars or additional training for information sharing on the current technological developments in the security systems or equipment for awareness improvement, monitoring of threat detection, and security features fragile infrastructures targets at nuclear facilities.

CONCLUSION

Cyber threats targeting nuclear facilities as critical infrastructure should have more attention. The advances in information

technology applied to critical infrastructure such as nuclear facilities increase their vulnerabilities. Moreover, their conditions are magnified by other causative factors such as environmental and social conditions as in the case of several attacks that have been reported. The risks could be worse than predicted when the hacker's ability for attacks critical infrastructure becomes more sophisticated. Thus, it was concluded that a strengthening program for nuclear cyber security could be performed through stakeholder collaboration involving intelligence role, resources support, training, and improvement of nuclear cyber capacity.

ACKNOWLEDGEMENTS

The authors declare that there is no conflict of interest regarding the publication of this article. This study has been supported by the Research Organization National Research and Innovation Agency of Indonesia and the State Intelligence College, State Intelligence Agency of Indonesia.

REFERENCES

1. Kim S, Heo G, Zio E, Shin J, Song J gu. Cyber attack taxonomy for digital environment in nuclear power plants. Nucl Eng Technol. 2020 May 1;52(5):995–1001.
2. Park J, Park J, Kim Y. A graded approach to cyber security in a research reactor facility. Prog Nucl Energy [Internet]. 2013;65:81–7. Available from: http://dx.doi.org/10.1016/j.pnucene.2013.01.007
3. Tripathi D, Singh LK, Tripathi AK, Chaturvedi A. Model based security verification of Cyber-Physical System based on Petrinet: A case study of Nuclear power plant. Ann Nucl Energy [Internet]. 2021;159:108306. Available from: https://doi.org/10.1016/j.anucene.2021.108306
4. Kim DY. Cyber security issues imposed on nuclear power plants. Ann Nucl Energy. 2014;65:141–3.
5. Office of Nuclear Reactor Regulation. Reading. 2007;1–3.
6. Collins S, McCombie S. Stuxnet: the emergence of a new cyber weapon and its implications. J Policing, Intell Count Terror. 2012;7(1):80–91.
7. Kenney M. Cyber-Terrorism in a Post-Stuxnet World. Orbis. 2015;59(1):111–28.
8. UHWO. Cyber Attack on German Nuclear Power Plant [Internet]. 2019. Available from: https://westoahu.hawaii.edu/cyber/regional/world-news-europe/cyber-attack-on-german-nuclear-power-plant/
9. BBC News. German nuclear plant hit by computer viruses [Internet]. BBC News. 2016. Available from: https://www.bbc.com/news/technology-36158606
10. Woo TH, Kwak SM. Social networking-based simulations for nuclear security: Strategy assessment following nuclear cyber terror on South Korean nuclear power plants (NPPs). Ann Nucl Energy [Internet]. 2015;81:91–7. Available from: http://dx.doi.org/10.1016/j.anucene.2015.03.016
11. Cho HS, Woo TH. Cyber security in nuclear industry – Analytic study from the terror incident in nuclear power plants (NPPs). Ann Nucl Energy. 2017 Jan 1;99:47–53.
12. Shin J, Son H, Heo G. Cyber Security Risk Evaluation of a Nuclear I&C Using BN and ET. Nucl Eng Technol [Internet]. 2017;49(3):517–24. Available from: http://dx.doi.org/10.1016/j.net.2016.11.004
13. Bowsher G, Milner C, Sullivan R. Medical intelligence, security and global health: the foundations of a new health agenda. J R Soc Med. 2016;109(7):269–73.
14. Uma M, Padmavathi G. A Survey on Various Cyber Attacks and Their Classification. Vol. 15, International Journal of Network Security. 2013.
15. Singh S, Silakari S. A Survey of Cyber Attack Detection Systems. Vol. 9, IJCSNS International Journal of Computer Science and Network Security.